

WHAT IS CLAIMED IS:

- 1                   1.       A system for multi-stream security processing and distributing  
2 digital media streams, the system comprising:  
3                   a headend configured to generate encrypted digital media streams;  
4                   a network coupled to the headend and configured to receive the  
5 encrypted digital media streams; and  
6                   at least one receiver coupled to the network and configured to receive  
7 the encrypted digital media streams and present a decrypted version of the encrypted  
8 digital media streams, wherein at least one of the headend and the at least one  
9 receiver comprises a security processor configured to provide at least one of  
10 simultaneous multiple encryption and simultaneous multiple decryption processing  
11 of the digital media streams.
- 1                   2.       The system of claim 1 wherein the media streams are at least  
2 one of a video stream, and audio stream, and a video plus audio stream.
- 1                   3.       The system of claim 1 wherein the security processor  
2 comprises a plurality of digital stream encryption/decryption engines that are  
3 selectively parallel coupled by a controller for simultaneous operation in response  
4 to a predetermined security configuration.
- 1                   4.       The system of claim 3 wherein the security configuration  
2 comprises at least one of Data Encryption Standard (DES), Triple DES (3-DES),  
3 Advanced Encryption Standard (AES), and Common Scrambling Algorithm (CSA).
- 1                   5.       The system of claim 3 wherein the security configuration  
2 comprises at least one of a secure download, RSA key management, multiple  
3 security key management, authentication, copy protection, and digital signatures.
- 1                   6.       The system of claim 3 wherein the security processor further  
2 comprises at least one of a memory containing a hash, engine encryption/decryption  
3 configuration logic, a random number generator, a multiplier, and a memory

4 containing a dynamic feedback arrangement scrambling technique (DFAST)  
 5 algorithm coupled in parallel to the controller and configured to provide multiple  
 6 key management for at least one of conditional access and digital rights  
 7 management.

1 7. The system of claim 3 wherein the security processor further  
 2 comprises at least one of a swappable random access memory (RAM) and a  
 3 swappable flash memory containing the predetermined security configuration.

1 8. The system of claim 3 wherein the security processor provides  
 2 role-based authentication that is used by an authorized user for at least one of  
 3 configuration, reconfiguration, and renewal.

1 9. The system of claim 1, wherein the receiver is at least one of  
 2 a set top box (STB), and a receiver or transceiver for at least one of digital  
 3 television, high definition digital television (HDTV), audio, MP3, text messaging,  
 4 and game digital streams.

1 10. The system of claim 1, wherein the receiver is a set top box  
 2 (STB) and the system further comprises an additional receiving device including the  
 3 security processor, coupled to the STB and configured to receive and decrypt the  
 4 encrypted digital media streams using the security processor.

1 11. A method of multi-stream security processing and distributing  
 2 digital media streams, the method comprising:  
 3 generating encrypted digital media streams at a headend;  
 4 coupling a network to the headend and receiving the encrypted digital  
 5 media streams at the network; and  
 6 coupling at least one receiver to the network and receiving the  
 7 encrypted digital media streams at the receiver, and presenting a decrypted version  
 8 of the encrypted digital media streams using the receiver, wherein at least one of the  
 9 headend and the at least one receiver comprises a security processor configured to

10 provide at least one of simultaneous multiple encryption and simultaneous multiple  
11 decryption processing of the digital media streams.

1 12. The method of claim 11 wherein the media streams are at least  
2 one of a video stream, and audio stream, and a video plus audio stream.

1 13. The method of claim 11 wherein the security processor  
2 comprises a plurality of digital stream encryption/decryption engines that are  
3 selectively parallel coupled by a controller for simultaneous operation in response  
4 to a predetermined security configuration.

1 14. The method of claim 13 wherein the security configuration  
2 comprises at least one of Data Encryption Standard (DES), Triple DES (3-DES),  
3 Advanced Encryption Standard (AES), and Common Scrambling Algorithm (CSA).

1 15. The method of claim 13 wherein the security configuration  
2 comprises at least one of a secure download, RSA key management, multiple  
3 security key management, authentication, copy protection, and digital signatures.

1 16. The method of claim 13 wherein the security processor further  
2 comprises at least one of a memory containing a hash, engine encryption/decryption  
3 configuration logic, a random number generator, a multiplier, and a memory  
4 containing a dynamic feedback arrangement scrambling technique (DFAST)  
5 algorithm coupled in parallel to the controller and configured to provide multiple  
6 key management for at least one of conditional access and digital rights  
7 management.

1 17. The method of claim 13 wherein the security processor further  
2 comprises at least one of a swappable random access memory (RAM) and a  
3 swappable flash memory containing the predetermined security configuration.

1 18. The method of claim 11 further comprising:  
2 presenting the encrypted digital media streams from the receiver; and

3 coupling an additional receiving device including the security  
4 processor to the receiver and receiving and decrypting the encrypted digital media  
5 streams at the receiving device using the security processor.

1 19. The method of claim 11 wherein the security processor  
2 provides role-based authentication that is used by an authorized user for at least one  
3 of configuration, reconfiguration, and renewal.

1 20. For use in a system for multi-stream security processing and  
2 distributing digital media streams, a security processor configured to provide at least  
3 one of simultaneous multiple media stream decryption and encryption processing,  
4 the security processor comprising:  
5 a controller; and  
6 a plurality of digital stream encryption/decryption engines that are  
7 selectively parallel coupled by the controller for simultaneous operation in response  
8 to a predetermined security configuration.

1 21. The security processor of claim 20 wherein the media streams  
2 are at least one of a video stream, and audio stream, and a video plus audio stream.

1 22. The security processor of claim 20 wherein the security  
2 configuration comprises at least one of Data Encryption Standard (DES), Triple  
3 DES (3-DES), Advanced Encryption Standard (AES), and Common Scrambling  
4 Algorithm (CSA).

1 23. The security processor of claim 20 wherein the security  
2 configuration comprises at least one of a secure download, RSA key management,  
3 multiple security key management, authentication, copy protection, and digital  
4 signatures.

1 24. The security processor of claim 20 wherein the security  
2 processor further comprises at least one of a memory containing a hash, engine  
3 encryption/decryption configuration logic, a random number generator, a multiplier,

4 and a memory containing a dynamic feedback arrangement scrambling technique  
 5 (DFAST) algorithm coupled in parallel to the controller and configured to provide  
 6 multiple key management for at least one of conditional access and digital rights  
 7 management.

1 25. The security processor of claim 20 wherein the security  
 2 processor further comprises at least one of a swappable random access memory  
 3 (RAM) and a swappable flash memory containing the predetermined security  
 4 configuration.

1 26. The security processor of claim 20 wherein the system for  
 2 multi-stream security processing and distributing digital media streams comprises  
 3 a headend, a network electrically coupled to the headend, a set top box (STB)  
 4 coupled to the network, and a receiver coupled to the STB, and the security  
 5 processor is implemented in connection with at least one of the headend, the  
 6 network, the STB, and the receiver.

1 27. The security processor of claim 20 wherein the security  
 2 processor provides role-based authentication that is used by an authorized user for  
 3 at least one of configuration, reconfiguration, and renewal.

1 28. The security processor of claim 20 wherein the security  
 2 processor is implemented in connection with a receiver or a transceiver that is at  
 3 least one of a set top box (STB), and a receiver or transceiver for at least one of  
 4 digital television, high definition digital television (HDTV), audio, MP3, text  
 5 messaging, and game digital streams.